

# METHOD FOR CONTROLLING ACCESS TO A NETWORK BY A WIRELESS CLIENT

## TECHNICAL FIELD OF THE INVENTION

5        This invention relates generally to secure network communication and, more particularly, to using a network address and configuration assignment process to dynamically establish a secure link, such as an IPSEC tunnel, between a wireless client and a network.

## BACKGROUND OF THE INVENTION

10        The broadcast nature of wireless communication makes it relatively easy for a person to "sniff" or monitor traffic on a wireless network to gain unauthorized access to it. One security measure that is currently available for wireless networks is requiring wireless clients to include a security code with each transmission. A  
15        problem with this measure is that there is nothing to prevent someone from ascertaining the security code by simply monitoring the transmissions from the client to the network. Another available security measure is the use of an encryption key for each group of users. However, if one member of a group compromises his or her copy of the key, or leaves the organization, then the entire group of users must be re-  
20        keyed in what is typically a time consuming process.

## SUMMARY OF THE INVENTION

In accordance with the foregoing, a method for controlling access to a network by a wireless client is provided. According to the method, an access point on the network receives a request for a network address broadcast by the wireless client.

- 5 The request is passed to an address server, which assigns a temporary address to the wireless client and provides the address of the access point. The wireless client then initiates a secure link with the access point based on the network address assigned by the address server and the address of the access point. If the secure link is not established before the temporary address expires, then wireless client is denied access
- 10 to the network.

Additional features and advantages of the invention will be made apparent from the following detailed description of illustrative embodiments that proceeds with reference to the accompanying figures.

## BRIEF DESCRIPTION OF THE DRAWINGS

While the appended claims set forth the features of the present invention with particularity, the invention, together with its objects and advantages, may be best understood from the following detailed description taken in conjunction with the accompanying drawings of which:

20 FIGURE 1 is a block diagram generally illustrating an example computer environment in which the present invention may be practiced;

FIG. 2 generally illustrates an example network in which the invention may be practiced;

FIG. 3 generally illustrates a more specific example of a network in which the invention may be practiced;

FIGS. 4-5 generally illustrate steps that may be taken to establish a secure link in accordance with an embodiment of the invention; and

5 FIG. 6 generally illustrates the network of FIG. 3 following the execution of the steps of FIGS. 4-5.

### **DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS**

Turning to the drawings, wherein like reference numerals refer to like  
10 elements, an exemplary environment for implementing the invention is shown in FIG. 1. The environment includes a computer 20, including a central processing unit 21, a system memory 22, and a system bus 23 that couples various system components including the system memory to the processing unit 21. The system bus 23 may be any of several types of bus structures including a memory bus or memory controller, a  
15 peripheral bus, and a local bus using any of a variety of bus architectures. The system memory includes read only memory (ROM) 24 and random access memory (RAM) 25. A basic input/output system (BIOS) 26, containing the basic routines that help to transfer information between elements within the computer 20, such as during start-up, is stored in the ROM 24. The computer 20 further includes a hard disk drive 27  
20 for reading from and writing to a hard disk 60, a magnetic disk drive 28 for reading from or writing to a removable magnetic disk 29, and an optical disk drive 30 for reading from or writing to a removable optical disk 31 such as a CD ROM or other optical media.

10

20

5  
10  
15

20

[illegible]

20

The invention is generally directed to a method for establishing secure communication with a wireless client. Referring to FIG. 2, a network set up in

5 The access point 102, address server 104 and computers 106, 108 and 110 are all linked by a network link 112. The network link 112 may be any of the alternatives described in conjunction with FIG. 1, including a wireless link. Although the network 100 is depicted as relatively small to aid in the description, it is understood that the invention may be practiced on any size network. Furthermore, it is understood that  
10 there may be multiple address servers on the network as well as multiple access points.

To gain access to the network 100, a wireless client 114 requests an address from the network via a wireless medium. The address server 104 responds by assigning a short duration address to the wireless client 114, and transmitting the assignment to the wireless client 114 via the access point 102. The address server 104 also transmits the network address of the access point 102 to the wireless client 114, preferably using the same packet as the network address assignment. The wireless client then establishes communication with the access point 102 and negotiates a secure link with the access point 102. Once a secure link has been established, the wireless client sends a request to have its network address renewed to the network 100 via the secure link. The address server 104 responds by renewing the address for a relatively long duration. The wireless client 114 may then communicate with any of the computers 106, 108 and 110 via the secure link.

Referring to FIG. 3, a more specific embodiment of a system set up in accordance with the teachings of the invention is shown. A network 200 includes a wireless access point 202 for allowing a computer to temporarily access the network 200 via a wireless link, a dynamic host configuration protocol (DHCP) server 204 for assigning internet protocol (IP) addresses and other network configuration values to devices on the network 200, and computers 206, 208 and 210. The wireless access point 202 is preferably a router, but may be any type of computer. The wireless access point 202, DHCP server 204, and computers 206, 208 and 210 are all communicatively linked by a network link 212, which in the illustrated embodiment is assumed to be an Ethernet link.

The wireless access point 202 may include a database 203 containing the MAC addresses of the wireless clients that are permitted to access the network 200 and an IP Security (IPSEC) module 205. In an embodiment of the invention, the database 203 may be generated by a network administrator. For example, if corporate employees need to access a corporate network via wireless medium, the network administrator could issue a wireless NIC to each employee and enter the MAC addresses of the cards into the database 203. The IPSEC module 205 sets up IPSEC tunnels with wireless clients. To ensure that no unauthorized users access the network 200, the access point 202 may, for example, not allow any network traffic from wireless clients to enter the network 200 unless the traffic originates from a MAC address listed in the database 203 and is either (1) transmitted through an IPSEC tunnel, (2) is a DHCP broadcast, or (3) is an initiation packet for an IPSEC



tunnel, such as an OAKLEY packet. OAKLEY (also known as IKE) is a well-known key exchange protocol.

A wireless client 214 is capable of communicating with the network 200 via a wireless medium. The wireless client 214 includes a wireless NIC 224, a wireless communicator 226, an application program 220 and a transport control protocol/internet protocol (TCP/IP) stack or module 222 having a transport control protocol/universal datagram protocol (TCP/UDP) layer 216, an internet protocol (IP) layer 218, an address resolution protocol (ARP) module 221, and an IPSEC module 223. The application program 220 sends and receives data through the TCP/IP module 222. The TCP/UDP layer 216 interprets and creates TCP and UDP headers for incoming and outgoing messages, while the IP layer 218 performs the same functions with respect to IP headers. The ARP module 221 generates ARP packets according to a well-known address resolution protocol. The IPSEC module 223 sets up security associations with other computers based on or more filter settings and encrypts or decrypts messages traveling to and from the other parts of the TCP/IP module 222. Such encryption may be carried out, for example, according to the well-known 3DES, DES, ECC, cryptographic algorithms and the like, and by using keys established as a result of Security association setup through the OAKLEY protocol. The IPSEC module 223 may also authenticate packets within messages using one or more well-known authentication algorithms, such as MD5 and SHA1. The NIC 224 acts as an interface between the TCP/IP module 222 and the communicator 226. Although not shown, the access point 202 may also have a TCP/IP module, wireless

NIC, and a wireless communicator whose functions are similar to those of the TCP/IP module 222, NIC 224 and communicator 226.

To access the network 200 in accordance with a preferred embodiment of the invention, the wireless client 214 obtains a limited duration IP address from the DHCP server 204, negotiates an IPSEC tunnel with the access point 202, and, once the IPSEC tunnel is established, renews the IP address for a relatively long duration.

Referring to FIGS. 4-6, a specific example of steps that may be followed to accomplish this procedure is shown. At step 300 of the flowchart of FIG. 4, the application program 220 on the wireless client 214 requests that a link be established with the network 200. The request is processed by the TCP/IP module 222, which generates a DHCP discover packet, and broadcasts the packet on the network 200 via the NIC 224 and the communicator 226 at step 302.

At step 304, the access point 202 receives the discover packet and examines its IP header. If the origin MAC address is not in the database 203, the access point 202 ignores the packet, thereby denying access to the network, and the procedure ends. If the origin MAC address is in the database 203, the access point 202 modifies the discover packet at step 306 by inserting data into an optional field of the packet to indicate that the packet originated from a wireless client. The access point 202 then transmits the modified discover packet to the DHCP server 204. At step 308, the DHCP server 204 responds to the discover packet with an ACK. The access point 202 relays the ACK to the client 214. At the client 214, the TCP/IP module 222 receives the ACK and responds to it by broadcasting a DHCP request packet via the NIC 224 and communicator 226 at step 310. At step 312, the access point 202

5 the modified packet to the DHCP server 304.

10

20

According to a specific embodiment of the invention, this policy is hard-coded into the NIC 224, so that the IPSEC module 223 need only fill in the source IP address, the destination IP address, and the destination MAC address. The IPSEC module 223 may also ensure that IPSEC components such as encapsulating security payload (ESP), the authentication header (AH) and such additional security measures as 3DES, MD5 and certificates or CERTS are used in when communicating from that assigned IP address.

At step 326, the ARP module 221 generates a gratuitous ARP packet using the MAC address of the NIC 224 and the IP address assigned by the DHCP server 204 in the source IP address header. The ARP packet is created as a broadcast packet whose destination is the network 200 and is sent to the IPSEC module 223. In response to receiving the ARP packet, the IPSEC module 223 initiates the process of setting up an IPSEC tunnel with the access point 202, using a protocol such as OAKLEY. The IPSEC module 223 then drops the ARP packet..

At step 328, the access point 202 determines whether there are currently any other clients using the same IP address as the wireless client 214 but using a different mac address than that of the wireless client, and that are using or negotiating the use of access point 202 as an IPSEC tunnel endpoint. If there are, then the flow proceeds to step 329, at which the access point 202 sends an ARP down each of these existing tunnels. The access point will also broadcast an ARP to the rest of the network 200 to determine whether there are any other clients in the network using the same IP address as the wireless client 214.

If any other client, wireless or otherwise, responds to the ARP, then the access point 202 denies the establishment of the tunnel. Otherwise, the flow proceeds to step 330, at which the access point 202 creates a static ARP entry for the wireless client 214 in a data structure 250 (FIG. 6). The entry contains the IP address to MAC address mapping for the wireless client 214. The access point 202 may also modify and reuse a previously existing static ARP entry, provided the tunnel originally represented by the entry is no longer valid. The access point 202 then negotiates with the wireless client 214 to set up an IPSEC tunnel 252.

Once the IPSEC tunnel 252 is established, the IP layer 218 of the wireless client 214 transmits a renewal request over the IPSEC tunnel. The access point 202 receives the renewal request packet, modifies it by inserting data into an optional field of the packet to indicate that the packet originated from an authenticated wireless client, and transmits the modified packet to the DHCP server. The DHCP server 204 receives the renewal request at step 332. If the lease on the IP address of the wireless client 214 has expired, then the DHCP server 204 informs the access point 202. The access point 202 then terminates the tunnel. Step 332 and its "YES" outcome may occur at any time after step 316, resulting in the termination of the process. At step 334, the DHCP server recognizes that the request came from an authenticated wireless client, and extends the lease on the IP address for a relatively long period of time - one day, for example. The process is then complete, and the wireless client 214 (FIG. 6) may now communicate with any of the computers 206, 208 and 210 via the IPSEC tunnel 252 and the access point 202.

It can thus be seen that a new and useful method and system for controlling access to a network by a wireless client has been described. In view of the many possible embodiments to which the principals of this invention may be applied, it should be recognized that the embodiments described herein with respect to the

5 drawing figures is meant to be illustrative only and should not be taken as limiting the scope of the invention. It should also be recognized that the various steps involved in carrying out the methods described above as well as the specific implementation of each step described above may be changed in ways that will be apparent to those of skill in the art.

10 Finally, those of skill in the art will recognize that the elements of the illustrated embodiment shown in software may be implemented in hardware and vice versa, and that the illustrated embodiment can be modified in arrangement and detail without departing from the spirit of the invention. Therefore, the invention as described herein contemplates all such embodiments as may come within the scope of  
15 the following claims and equivalents thereof.

009290-5672950  
09507195-062300